MECHANISM FOR DETECTION OF ATTACKS BASED ON IMPERSONATION IN A WIRELESS NETWORK

Field of the invention

[001] The invention is directed to intrusion detection systems and in particular to a mechanism for detection of attacks based on impersonation in a wireless network.

Background of the invention

[002] Wireless Networks have become more and more prevalent over the past few years as they appeal to the end users for the convenience they provide.

[003] Security is an issue in this kind of network as the communication media used is shared. As a result, wireless networks are particularly vulnerable to attacks at the lowest levels of the communication protocols (first and second layer of the OSI model). It is indeed very easy to tap or inject traffic into such a network.

[004] Such attacks could be used to impersonate a wireless node in order to gain a fraudulent access to the network or, even more dangerous, to arbitrary create denial of services, or 'man in the middle' attacks by impersonating nodes that assume a special function in the network (i.e. an access point in an 802.11 network).

[005] Traditional security systems and technologies such are firewall or IPSec tunnel fail to fully address those threats since they are not designed to address security threats at lower levels of the OSI model. Other mechanisms, such as address filtering performed by the wireless equipment, are useless in this environment where impersonating a valid address is so easy to do.

[006] It is now well understood by the industry that solutions that monitor the wireless traffic to detect the above mentioned attacks bring security

benefits. This explains the increasing appearance of Intrusion Detection System (IDS) in the wireless product space.

[007] An IDS is an entity on a network that monitors a variety of system and network resources for anomalies to detect attempts to compromise the network. An IDS generally assesses if the monitored data satisfies the network rules and heuristics, mismatches indicating an attack in progress. The IDS will then advise the network user of the attack; more sophisticated IDS may launch automatic network defense counter-measures. Monitoring can take many forms and spans from low-level inspection of the data source and destination, to inspection of data packets content and monitoring the activity on a specific host.

[008] These security services are especially important for wireless communication, due to the ease of tapping into wireless networks. In addition, since firewalls are employed on the user side of a wireless link, a message rejected by the firewall has already consumed the wireless resources required to transmit. The wireless links are supported by RF channels, which are a scarce resource. Accordingly, messages rejected by the firewall tend to waste bandwidth which could be allocated to other connections, can drive up user cost by increasing message transmissions, and tend to slow overall throughput because of the resources required to transmit them over the wireless link.

[009] A specificity of wireless networks is that they require IDS-like systems specific to the lower MAC layer management element (as defined by the seven-layer OSI model) while traditional IDS systems mainly focus on the third and higher layers of the OSI model.

[0010] US patent Application 2003/0135762 (Macaulay) entitled "Wireless Network Security System" and published July 17, 2003, discloses an 802.11 security system for monitoring wireless networks for detecting and locating unauthorized or threatening IEEE 802.11 devices entering a user's wireless network environment or a facility not intended to support wireless networks. The security system comprises a network appliance subsystem, a portable computing subsystem and an interface between

these two subsystems. The portable computing subsystem is a manually operated device, which searches for specific devices using a directional antenna and indicates when targeted (intruder) radio signals are found, and the signal strength. The network appliance subsystem is equipped with an analyzing module that looks for IEEE 802.11-specific attack patterns using real-time analysis, and contains configurations related to alert levels and security policy configurations. However, this solution relies on traffic monitoring to detect intrusion and requires duplication of all wireless interfaces used by a respective node.

[0011] In addition, existing wireless IDSs, such as the Guard product by AirDefense™, rely on a set of network probes and a specific server appliance. However, there is no correlation or consolidation between the wireless node and the IDS system.

[0012] Joshua Wight describes in an article entitled "Detecting Wireless LAN MAC Address Spoofing", publication date not provided, available at http://www.polarcove.com/whitepapars/detectwireless.pdf, provides an in-depth analysis of the anomalies generated by tools that spoof MAC addresses. While knowledge of these anomalies enables an easier detection of the spoofed traffic generated by these tools, the analysis has some limitations. For example, it is based on anomalies generated by specific attack tools, which should not be considered as invariants. As well, most of the anomalies are present when random MAC addresses are used for attacks, which is not always the case.

[0013] In general, the prior art solutions rely only on wireless traffic monitoring in order to detect intrusions. Using such techniques, it is not possible to differentiate in a reliable way the legitimate traffic sent by a node (for instance the management or control frames) from the malicious traffic generated by an attacker node masquerading as the real node.

[0014] This inability to detect in a reliable way the occurrence of malicious traffic leaves wireless nodes susceptible to various types of attacks such as de-authentication, some Man in the Middle, denial of service, etc.

Summary of the Invention

[0015] It is an object of the present invention to provide a mechanism for the detection of attacks based on impersonation in a wireless network.

[0016] It is another object of the invention to increase the protection of a wireless node against the class of attacks based on impersonation of a node using the physical address or other higher layer address.

[0017] Accordingly, the invention provides a method for detecting impersonation based attacks at a wireless node of a wireless communication network, comprising the steps of: a) providing an intrusion detection module with a copy of original data frames transmitted by the wireless node over a wireless interface; b) detecting at the intrusion detection module incoming data frames received over the wireless interface; and c) recognizing an impersonating attack when the information in the copy differs from the information in the incoming data frames.

[0018] The invention is also directed to an impersonation detection system for a wireless node of a wireless communication network, the node for transmitting original data frames over a wireless interface comprising: an intrusion detection module for correlating the original data frames with incoming data frames received over the air interface; and connection means between the wireless node and the intrusion detection module for providing the intrusion detection module with a copy of the original data frames.

[0019] Still further, the invention is directed to a wireless node for a wireless network comprising: means for transmitting outgoing data frames over a wireless interface; an intrusion detection module for correlating the outgoing data frames with incoming data frames received from the air interface; and a secure link between the wireless node and the intrusion detection module for providing the intrusion detection module with a copy of the outgoing data frames.

[0020] Advantageously, the detection mechanism according to the invention provides reliable detection of attacks based on impersonation of a

wireless node, while it does not require any specialized, costly equipment. Minor changes in the wireless node implementation are required to publish appropriate information to the intrusion detection module; however these changes are fully offset by the increased intrusion detection reliability.

[0021] As well, it does not require any change to any wireless networking standard to operate.

[0022] This invention does not provide a full IDS solution for wireless networks, but rather aims to solve a problem, which cannot normally be solved by the existing IDS solutions.

Brief Description of the Drawings

Figure 1 illustrates the logical architecture of an impersonation detection system according to an embodiment of the invention; and
Figure 2 shows the attack detection process performed using the detection system of Figure 1.

Detailed Description of the Invention

[0023] This invention proposes to exploit additional information made available by the wireless node in order to enhance the intrusion detection capabilities of the wireless networks. The invention comprises an intrusion detection module connected to the wireless node under surveillance by a secure link. The wireless node sends to the intrusion detection module a copy of the traffic it sent to the wireless interface over the secure link.

[0024] For increased efficiency, this copy may not encompass all traffic processed by the wireless node. For instance, in a 802.11 network, it may only consist of management frames which by themselves enable the detection of a large variety of attacks. It may also be a summary of the traffic, which would allow statistical comparisons to be made such as differences in the number and types of the frames.

[0025] This intrusion detection module monitors the traffic transmitted over the wireless interface by the wireless node and compares it to the information about the same traffic as sent by the wireless node over the secure link. Any inconsistencies between the wireless traffic received and the information received would show suspect behavior that can be analyzed to qualify the attack. For example, if a monitored wireless node is inactive but the intrusion detection module receives wireless traffic that indicates the monitored node is the originator, then this would be a sign of suspect behavior.

[0026] Figure 1 illustrates the logical architecture of the impersonation detection system **1** according to the invention. It shows a node **10** of a wireless communication network and an intrusion detection module IDM **20** connected to node **10** over a secure link **30**. System **1** includes a respective transmitter unit **15** at node **10**, connected to a receiver unit **25** at intrusion detection module **20** over secure link **30**, operating according to a respective communication protocol. The language used for the exchange of information over the secure link **30** could be standardized for a better openness and for easing integration with third party intrusion detection systems available for wireless networks.

[0027] It is to be noted that the blocks shown in Figure 1 represent the logical components of the impersonation detection system. Indeed, these blocks may be integrated in order to build a wireless node with embedded impersonation detection capabilities. In this case, the secure link between node **10** and module **20** could be replaced by inter-processes communications.

[0028] Node **10** generates original data denoted with **A**, which is modulated over the wireless channels that are allocated to node **10**, as well known, and an antenna **12** transmits wireless traffic **a** over wireless interface **14**. This transmission is performed in the normal fashion for the wireless technology in question; the transmission technology is not relevant to this invention. Node **10** also sends a copy of the original data **A** to the intrusion detection module **20** over the secure link **30**. As indicated

above, this copy may include only management frames, or a summary of the traffic.

[0029] The intrusion detection module **20** monitors the channels allocated to node **10** using an antenna **22**. It collects wireless traffic denoted with **b** on Figure 1, and a receiver **26** detects data **B** carried by these channels. A data processing unit DPU **28** at IDM **20** correlates data set **A** and data set **B**; an intrusion is detected when data set **C** is not empty.

[0030] Note that if the copy of the original data **A** encompasses only selected frames of the traffic processed by the wireless node, DPU **28** selects for correlation similar frames from incoming data **B**.

[0031] The output of DPU **28** may be used as such to alarm the node or the network management system of an intrusion. This information may also be used in conjunction with information gathered by any wireless intrusion detection system available in the respective network, and used as a means to achieve a better diagnosis of attacks going on in the wireless network.

[0032] Figure 2 shows the attack detection process performed using the detection system of Figure 1. As indicated above, DPU **28** (see Figure 1) uses data **A** corresponding to the wireless traffic **a** sent by the wireless node **10** and the incoming data **B** corresponding to the wireless traffic **b** received by the intrusion detection module **20**. In step **40**, DPU **28** correlates these two sources of information in order to detect spoofed traffic that uses the physical address on node

[0033] If the result **C** of the subtraction of the set **A** to the set **B** is not empty, as shown by branch 'No' of decision block **41**, this means that an impersonation attack is going on, shown in step **42**. Further analysis could be used to obtain a more accurate assessment of the attack according to the wireless protocol monitored. For instance, in the case of an 802.11 network, the detection of a forged de-authentication or disassociation 802.11 management frame can allow detection of a denial

of service attack. A 'man in the middle' attack can be diagnosed, if such a packet is followed by an association to another wireless node.

[0034] Conversely, if the result **C** of the subtraction of the set **A** to the set **B** is empty, as shown by the 'Yes branch of decision block **41**, this means that no attack has been detected, shown in step **43**.

[0035] The embodiments and variations shown and described herein are merely illustrative of the principles of this invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention.